Toward SVOPME, a Scalable Virtual Organization Privileges Management Environment

Nanbor Wang[1], Gabriele Garzoglio[2], Balamurali Ananthan[1], Steven Timm[2]

[1] Tech-X Corporation, 5621 Arapahoe Ave, Suite A, Boulder, CO 80303, USA
[2] Fermi National Accelerator Laboratory, P.O. Box 500, Batavia, IL, 60510, USA

garzoglio@fnal.gov

Abstract. Grids enable uniform access to resources by implementing standard interfaces to resource gateways. In the Open Science Grid (OSG), privileges are granted on the basis of the user's membership to a Virtual Organization (VO). However, user privilege definitions and enforcements are administered separately by VOs and Grid sites. Such partitioning can potentially introduce inconsistent user privileges throughout the Grid and break the Grid paradigm of uniform access to resources. There is a need for an automated privilege management mechanism for a VO to codify privilege policies granted to its users, to propagate the policies to grid sites, to identity and suggest remedies for non-supported VO privileges at individual sites. The Scalable Virtual Organization Privileges Management Environment (SVOPME) addresses the challenge under the context of the Open Science Grid (OSG). The SVOPME provides tools for VOs to define and publish desired privileges. At a site, SVOPME tools help analyze access policies defined for VO users and verify policy consistency between VOs and sites, and suggest site configurations changes. This paper presents the designs and features of SVOPME tools and the lessons learned in applying SVOPME tools for OSG VOs and sites. Furthermore, we will outline future improvements to SVOPME tools to adapt to a range of different site configurations and new privilege policies.

1. Introduction

The Grid computing environment has emerged as the leading technology for coordinated resource sharing among participating institutions and individuals. It enables execution of large-scale computation jobs by providing uniform access to distributed resources such as computational cycles and data storage, shared among participating institutes. The Virtual Organization (VO) is a key concept in grid computing. A VO manages members from different home institutes with common interests. Multiple VO's can coexist and share a common set of resources in a Grid. Meanwhile, the structure and membership of a VO are dynamic, as groups and individuals may join and leave VO's based on their interests and needs.

1.1. Challenges in Reconciling VO and Site Policies

Within a Grid body such as the Open Science Grid (OSG) [1] or European Grid for E-sciencE (EGEE) [2], a VO establishes resource-usage agreements with Grid resource providers to grant access of site resources to group of users within a VO. Modern Grid middleware provides both the mechanisms and tools to enable the fine-grained, role-based access control. However, it comes up short in providing a streamlined and consistent distributed user privilege management capability across VO's and sites. Currently, this lack of policy definition, distribution, and reconciliation mechanisms is handled manually via verbal discussions between VO administrators and site administrators. Such manual propagation of VO policies is a brittle and time-consuming process. As privilege policies change dynamically, which is becoming more common for large VO's, and new VO's come onboard, Grid utilization suffers as legitimate users may not be able to access resources which are otherwise perfectly usable.

1.2. The Need for Managing VO User Privileges
To realize the vision of providing uniform access to distributed resources in Grid Computing, there is an urgent need to bridge the gap between VO privilege policy specifications and local Grid site configurations. VO user roles and privilege policies must be able to propagate to Grid site automatically, yet allowing site administrators to retain full control over site policies. Furthermore, with the ever changing numbers of VO's, organizations, and privilege policies, there need to be tools to help both VO and site administrators to verify that policies at VO's and sites are consistent with one another.

2. Related Works
SVOPME project is synergistic to many projects on authorization management. For example, the GPBox [3] project is a policy management framework for the Grid environment to globally modify the execution priorities of jobs submitted from VOs at sites. Compared to GPBox, SVOPME project does not attempt to configure site policies directly. Instead, SVOPME produces compliance reports about local configurations that hint on how the configurations could be modified for the site to provide better support for VO's. We believe that leaving local site administrators in full control of site configuration will give them peace of mind and reduce their reservation toward the eventual adoption of SVOPME.

Another effort closely related to SVOPME is the Authorization Interoperability project [4]. This project defines an attribute and obligation profile for authorization interoperability across Grids as described in Section 3. We will leverage the efforts from this project to integrate SVOPME into OSG and other Grid infrastructure.

3. VOs and Grid Sites Policies
Figure 1 illustrates the security model in OSG. A user authenticates with the VO and obtains a signed assertion of membership. This assertion is presented to the Grid site for authorization.

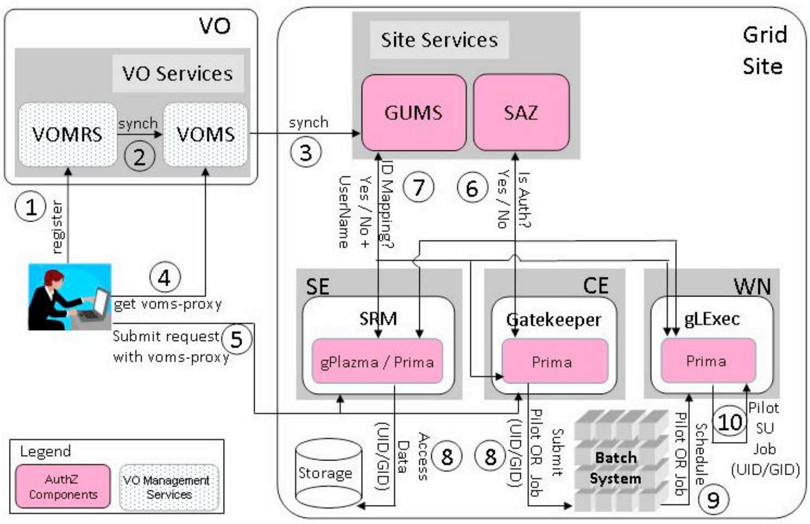

Figure 1: The OSG Security Model.

The Authorization Interoperability project [5] standardizes the terms and formats used in the authorization process between security components, specifically Policy-Enforcement-Point (PEP), such as a Globus Gatekeeper, and Policy-Decision-Point (PDP), such as GUMS [6]. This profile is based on the eXtensible Access Control Markup Language (XACML) [7] and the Security Assertion Markup Language (SAML) [8]. However, as highlighted by Figure 1, the existing Grid security model does not provide support for a policy-administration-point (PAP), i.e., how a VO can define its privilege policies. The SVOPME project, therefore, fills this gap and utilizes XACML as its VO privilege policy definition language for administering policies over the Grid.

4. The SVOPME Architecture

SVOPME addresses the challenges in administering and maintaining user privileges over multiple VOs and grid sites. Figure 2 illustrates the architecture of the SVOPME and the interactions among SVOPME tools. Four key components (round blue boxes in Fig 2) provide the core functionality of SVOPME. They include support for VO administrators to define and generate VO privilege policies, and for site administrators to automatically generate local site privilege policies based on existing site configurations.

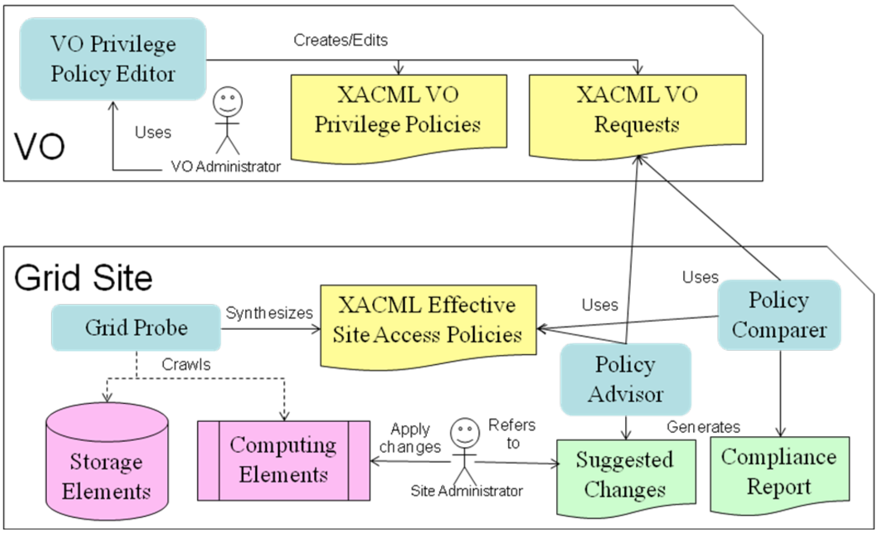

Figure 2: Overall SVOPME Architecture.

To allow easy extension of the policies supported, we designed the tools to use policy templates. The use of policy templates allows us to support new policy types by simply adding new templates into the tools chain without modifying the core implementations. The remainder of this Section describes these tools in more details.

4.1. VO Components

Figure 3 illustrates all the utilities that SVOPME provides for VO administrators. In the core of VO support tools is the XACML VO Policy Editor. As we mentioned earlier, the VO Policy Editor uses XACML as the internal representation of privilege policies. This provides a generic mechanism for describing, combining, and reasoning with policies. Since XACML as a language is too complex and verbose for VO administrators to express their policies, the VO community, therefore, needs to define a vocabulary (i.e., XACML profile) to frame the concepts in its domain and VO administrators may not be expert in it.

In order to address these issues, we have developed a “domain-specific” GUI-based VO policy editor. The editor enables VO users to create individual privilege policies as separate XACML files. For every VO policy defined by the VO Policy Editor, a matching XACML verification request is generated. These requests define the operations that must be permitted at a Grid site supporting the

VO and are used to test the compliance of Grid sites. A "Request Archiver" packages all these test queries into a time-stamped archive, which can then be published on the VO's web site. Timestamps allow other tools ("Site Components" sec.) to retrieve only the latest set of test queries.

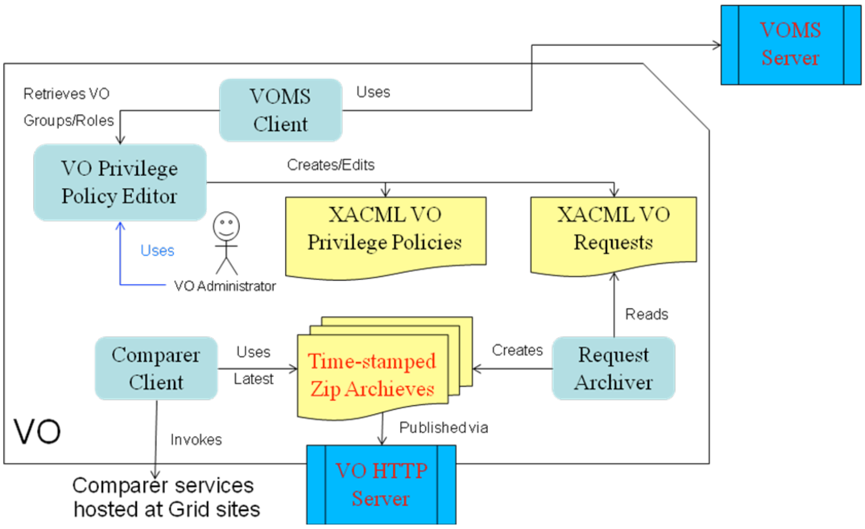

Figure 3: VO Tool interactions.

The "Comparer Client" provides VO administrators and users access to the policy comparer Web Service hosted on Grid sites. Users can use the comparer client contact to verify the degree of VO privilege support at individual sites using a set of test requests.

4.2. Site Components

This Section describes the 3 site-specific components in SVOPME, namely, Grid Probe, Policies Advisor, and Policies Comparer as shown in Figure 4.

4.2.1. *Grid Probe*: Mechanisms for enforcing Grid site privilege policies currently are scattered at different locations on a Grid site. There is no one centralized entity to manage and configure existing Grid middleware infrastructure. To try to compare and reason on VO policies directly with all these configuration points will result in ad hoc software tools that are very complicated and hard to maintain and expand.

The Grid Probe addresses this issue by scanning and gathering configuration information from various tools and mechanisms at a Grid site. The Grid Probe then analyzes this information and generates the *effective local privilege policies* in XACML.

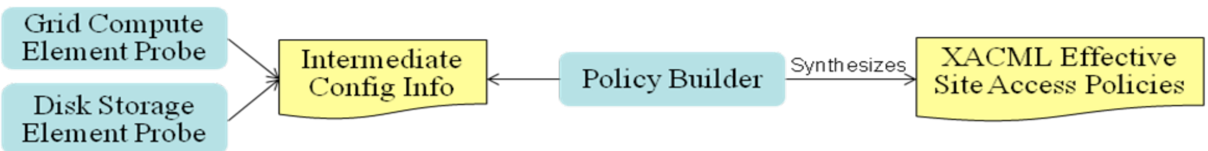

Figure 4: SVOPME's site mechanisms for synthesizing effective site policies.

4.2.2. Analyzing Site Configurations: SVOPME uses the verification queries generated by the VO policy editor to verify if policies defined by a VO are supported on a site. Using the VO Request Retriever, the site checks periodically if a VO has published a new set of verification queries, and downloads them when necessary. As shown in Figure 5, the requests for VOs are cached locally at Grid sites and are used to verify the site configurations as described in the remainder of this Section.

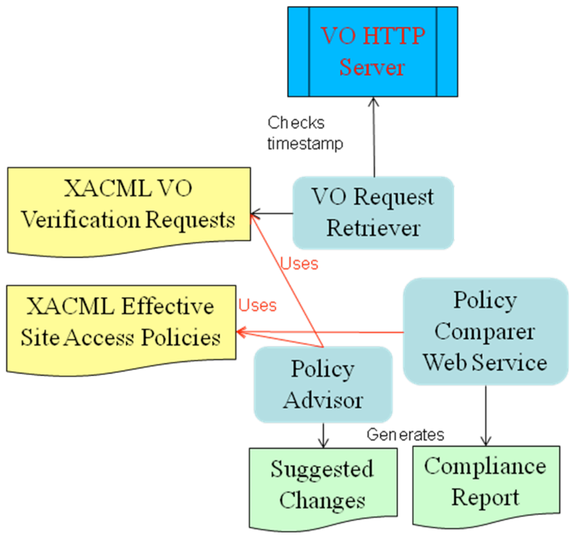

Figure 5: VO requests are used to verify site configurations.

4.2.3. *Policy Advisor*: The Policy Advisor runs on Grid sites. It verifies if the VO privilege policies are supported at the site by testing VO verification requests against the local privilege policies, generated by the Grid probe. The Policy Advisor also maintains a collection of site configuration guidelines based on experiences of site administrators using the type of resources and configurations. If the site fails to comply with a specific policy, the Policy Advisor will analyze and recommend a way to modify the site configuration to correct the problem using the knowledge base.

4.2.4. *Policy Comparer*: The Policy Comparer is a Grid Service invoked by a VO administrator or any VO user to verify the degree of support of the site of their VO privilege policies. Site compliance test can be done by using the Policy Comparer Client VO tool with a set of test queries to check if the VO policies are supported at the site. By providing the Policy Comparer Web Service, we avoid publishing the site configurations information in the form of site equivalent policies while allowing the VO users to verify site compliance by producing a pass/fail response to each query.

5. Experimental Deployments

We have deployed the SVOPME tools in a realistic, large-scale Grid environment using FermiGrid's integrated test bed (ITB). To evaluate the effectiveness of SVOPME, we gathered and defined the VO policies for the DZero and the Engage VO's of OSG. The experiment motivated several enhancements in Grid tools. Furthermore, we were able to identify some inconsistent and unconventional site configurations in our target site environment.

Some of the differences are due to legacy site configurations known to the administrators. More importantly, SVOPME was able to identify some inconsistencies in the ITB that were unknown to the site administrators. This experiment demonstrated the potential benefits brought by SVOPME to managing a Grid. If deployed in large scale, we believe that we will be able to further demonstrate how the SVOPME project addresses the scalability issues in providing consistent resource usage over the Grid.

6. Conclusions

To address the scalability issues in providing consistent access to Grid resources, we have developed a set of tools and services to realize a Scalable Virtual Organization Privilege Management Environment. We have demonstrated the feasibility and the effectiveness of this project in a test bed environment to allow VOs and sites to communicate the VO privilege policy needs and to verify the degree of site support automatically. Fully deployed, the SVOPME project can greatly reduce the costs in running and maintaining VO's and sites alike. Similarly, SVOPME allows sites to advertise and prove their degree of support for a VO. SVOPME provides semi-automatic mechanisms to amend site configurations so that a site can easily support a new VO and its privilege policies. Equally important is that Grid sites do not relinquish the privilege enforcement to the VOs. Rather, SVOPME informs the site administrators with a formal VO policy assessment.

We intend to have SVOPME incorporated in the Virtual Data Toolkit (VDT), the *de facto* standard Grid middleware distribution. Currently, we are actively recruiting more VOs and Grid sites to perform "field tests" in a production environment. We also plan to extend SVOPME to help ensure that VOs and Grid sites have a uniform set of security policies.

Acknowledgments
This work is partially funded by the Office of Advanced Scientific Computing Research, Office of Science, United States Dept. of Energy under contracts DE-FG02-07ER84733 and DE-AC02-07CH11359, the Fermi National Accelerator Laboratory, and the Tech-X Corporation.

References

[1] Pordes R et al. 2007 The Open Science Grid *Journal of Physics: Conference Series* 78 15
[2] Laure E et al. 2004 Middleware for the next generation Grid infrastructure *Proceedings of Computing in High Energy Physics and Nuclear Physics 2004*, Interlaken, Switzerland 826
[3] Cesini D, Ciaschini V, Dongiovanni D, Ferraro A, Forti A, Ghiselli A, Italiano A, Salomoni D 2008 Enabling a priority-based fair share in the EGEE infrastructure *Journal of Physics: Conference Series* 119 062023 DOI:10.1088/1742-6596/119/6/062023
[4] Garzoglio G et al. 2009 Definition and Implementation of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware in OSG and EGEE *Journal of Grid Computing* DOI: 10.1007/s10723-009-9117-4
[5] Garzoglio G et al. 2008 An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids *Fremilab White Paper* CD-doc-2952-v2
[6] Lorch M, Kafura D, Fisk I, Keahey K, Carcassi G, Freeman T, Peremutov T, Rana A S 2005 Authorization and account management in the Open Science Grid *The 6th IEEE/ACM International Workshop on Grid Computing,* 2005
[7] Moses T et al. 2005 Extensible access control markup language (xacml) version 2.0 *Oasis Standard*
[8] Cantor S, Kemp J, Philpott R, Maler R 2005 Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2. 0 *OASIS SSTC*